REMARKS

Claims 1-22 remain in the application and stand rejected. Claims 1, 18, and 21 have been amended to correct obvious typographical errors.

Reconsideration of the rejection is respectfully requested in light of the following reasons.

Claim Rejections -- 35 U.S.C. § 102 (Chen)

Claims 1-5, 7-11, 13, and 14 stand rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 6,061,796 to Chen et al. ("Chen"). The rejection is respectfully traversed.

Claim 1 is patentable over Chen at least for reciting: "in a data transfer between the first peer node and the second peer node" and "receiving the data in the interception node." That is, claim 1 requires the data to be transferred between two peer nodes to be received in the interception node. In Chen, the authentication server provides authentication services and is thus passed authentication information by the shim 50. However, data to be transferred between peer computers do not pass through the authentication server ("interception node") or any node on the network whose location information has been substituted for that of the destination computer (Chen, FIG. 6, channel 62; col. 11, line 59 to col. 12, line 19). For example, Chen is explicit that:

> "...the peer-to-peer applications are designed only to communicate with "peers" 45 and **not with the authentication server**..."

Chen, col. 9, lines 62-64 (emphasis added)

In other words, in Chen, data to be transferred between two peer nodes are directly transferred between the peer nodes. This creates a serious problem as direct data transfer between peer nodes may result in proliferation of computer viruses (e.g. see Specification, page 3, lines 3-9).

Chen col. 11, lines 24-49, cited in the rejection of claim 15, explains the role of the authentication server in a peer-to-peer communication. In the case where clients

communicate **over a direct link 62** (see Chen, FIG. 6), the authentication server opens a secured channel 63 to an authentication client software to perform an authentication procedure and transmit **session keys** for decrypting communications sent over the channel 62 (the direct link where data transfer is performed). Note that only authentication communications pass through the authentication server; in peer-to-peer communications, data transfer is over a direct channel 62.

Claim 1 is further patentable over Chen at least for reciting: "**providing** the second peer node a location information of an interception node **instead** of a location information of the first peer node in a data transfer between the first peer node and the second peer node" (emphasis added). Chen discloses a virtual private network with centralized authentication services for peer nodes. In Chen, the socket shim 50 is used to intercept function calls (Chen, col. 9, lines 42-59) to allow for authentication by an authentication server. Chen is explicit that:

> "Since the basic authentication client software is designed to send all communications directly to the authentication server, while the peer-to-peer applications are designed only to communicate with 'peers' 45 and not with the authentication server, **the principal function of shim 50 is to arrange for the destination of address of the communication to be supplied to both the authentication client software and to authentication server**, even though the peer application assumes that it is communicating only with the peer application."
>
> Chen, col. 9, line 60 to col. 10, line 2 (emphasis added)

That is, in Chen, the sender computer is not provided the location information of the authentication server (or another server) instead of that of the receiving computer. In fact, in Chen, **the sender computer must send the authentication server computer the address of the receiving computer**. This point is reiterated in Chen's Abstract:

> "Where the parties to the communication are peer-to-peer applications, the intercepted function calls, requests for service, or data packets include **the destination address of the peer application, which is supplied to the server** so that the server can authenticate the peer and enable the peer to decrypt further direct peer-to-peer communications."
>
> Chen, Abstract (emphasis added)

This is opposite to what is recited in claim 1, where the second peer node is expecting to be provided the location information of the first peer node but is instead provided the location information of the interception node.

For at least the above reasons, it is respectfully submitted that claim 1 is patentable over Chen.

Claims 2-5 and 7-9 depend on claim 1 and are thus patentable over Chen at least for the same reasons that claim 1 is patentable. For example:

Claims 2 and 3 recite that the data being transferred between the first node and the second peer node (claim 1) are received by the interception node from the second peer node (claim 2) or the first peer node (claim 3). Chen does not disclose or suggest data to be transferred between two peer nodes to be transmitted through an interception node whose address has been substituted for that of the destination peer node.

Claim 4 recites that the data being transferred between the first peer node and the second peer node (claim 1) and received in the interception node comprise a file. Chen cannot meet the limitation of claim 4 because Chen does not disclose or suggest file transfer except between peer nodes. That is, in Chen, the authentication server only performs authentication functions – files transferred between peer nodes are not redirected to the authentication server or any server whose address has been substituted for that of a destination peer node.

Claim 7 recites that the contents of the data are filtered **in the interception node**. Chen, col. 9, lines 42-59, cited in the rejection of claim 7, discusses the functionality of the shim 50, which is in a client (Chen, FIG. 3) and not in the authentication server ("interception node"). Chen does not disclose or suggest filtering the contents of data to be transferred between two peer nodes in the authentication server. As explained above, filtering of data in the authentication server is suspect given that data transfer does not even go through the authentication server in the first place. Filtering of data in Chen's authentication server is further suspect given that data being transferred is

encrypted and can only be decrypted in a peer node. In Chen, the encryption and decryption are performed in the sending and destination computers (Chen, FIG. 7, steps 106 and 109; col. 12, lines 11-26; Abstract), not in the authentication server. The authentication server merely provides session keys to peer nodes.

Claims 8 and 9 recite that the data being transferred between the first peer node and the second node are transferred from the interception node to the second peer node (claim 8) or the first peer node (claim 9) after processing in the interception node. Chen does not disclose or suggest data to be transferred between two peer nodes to be transmitted through an interception node for processing, the interception node having location information that has been substituted for that of the first peer node.

Claim 10 is patentable over Chen at least for reciting: "redirecting the file from a first peer node to an interception node, the file being originally intended to be transferred directly from the first peer node to a second peer node." As explained above in regard to claim 1, files to be transferred between peer nodes are NOT redirected in Chen. In Chen, file transfer can only occur between peer-to-peer applications in peer nodes (Chen, col. 9, lines 62-64, col. 10 lines 2-4; FIG. 6, channel 62).

Chen col. 6, line 66 to col. 7 line 15 discusses the functionality of the shim 50, which intercepts **function calls** to redirect **initial communications** to establish a secured communication. Nothing in that cited section discloses or suggests redirecting to the authentication server files to be transferred between two peer nodes. On the contrary, as explained above, peer nodes perform direct data transfer in Chen.

For at least the above reasons, it is respectfully submitted that claim 10 is patentable over Chen.

Claims 11, 13, and 14 depend on claim 10 and are thus patentable over Chen at least for the same reasons that claim 10 is patentable. For example,

Claim 13 recites that the **content of the file** is filtered **in the interception node**. Chen, col. 9, lines 42-59, cited in the rejection of claim 13, discusses the functionality of the shim 50, which is NOT in the authentication server

("interception node") in the first place. Chen does not disclose or suggest **filtering** the content of a file in the authentication server. In Chen, files to be transferred between two peer nodes do not even pass through the authentication server.

Claim 14 recites: "informing the second peer node that an address of the first peer node is that of the interception node." In the rejection of claim 14, the last office action suggests that Chen, in col. 12, lines 11-32, discloses the aforementioned limitation. This conclusion is respectfully traversed in that Chen, as explained above, relies on a shim to perform interception of authentication information, not files being transferred between two peer nodes. The cited section of Chen describes the method of FIG. 7, which involves the client program 20 receiving the destination peer address, which is eventually provided to the authentication server upon interception by the shim. However, the sending computer is **not informed that the address of the receiving computer is that of the authentication server**, as required by claim 14. In Chen, the sending computer needs a shim that provides the location information of the destination computer to the authentication server instead of the other way around. Therefore, it is respectfully submitted that claim 14 is patentable over Chen.

Claim Rejections -- 35 U.S.C. § 102 (Yeager)

Claims 16 and 19 stand rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Publication No. 2003/0028585 by Yeager et al. ("Yeager"). The rejection is respectfully traversed.

Claim 16 is patentable over Yeager at least for reciting: "the presence modifier being configured to provide to a second peer node a location information of an interception node **instead of** the location information of the first peer node **in response to** a detection of the publication" (emphasis added). Yeager pertains to trust mechanisms in peer-to-peer networks. However, Yeager does not disclose or suggest a presence modifier providing a peer node location information of an interception node instead of

the location information of another peer node in response to detection of the publication of the location information of the peer node.

Yeager paragraphs [0013], [0162], and [0173] are cited in the rejection of claim 16. Yeager paragraph [0013] discusses peer-to-peer networks in general. Yeager paragraph [0162] introduces the concept of peer-to-peer authorization services and publication of addresses for authorization peers. Yeager paragraph [0173] discloses that a certificate on a key ring may include a peer identifier, the address of the certificate's subject or owner, and the local peer's certificate confidence for that certificate. None of the cited paragraphs discloses or suggests providing a second peer node the location information of an interception node **instead of that of a first peer node** in response to detection of the publication of the location information of the first peer node. The Yeager trust mechanisms have nothing to do with substituting an address of an interception node for that of a peer node, let alone doing so in response to a publication of the location information of another peer node. Therefore, it is respectfully submitted that claim 16 is patentable over Yeager.

Claim 19 depends on claim 16 and is thus patentable over Yeager at least for the same reasons that claim 16 is patentable.

Claim Rejection -- 35 U.S.C. § 103 (Chen and Joiner)

Claims 6 and 12 stand rejected under 35 U.S.C. §103 as being unpatentable over Chen in view of U.S. Patent No. 6,789,117 to Joiner et al. ("Joiner"). The rejection is respectfully traversed.

Claim 6 depends on claim 1 and claim 12 depends on claim 10. The patentability of claims 1 and 10 over Chen has already been explained above. Joiner does not add anything to Chen in regard to claims 1 and 10. Therefore, it is respectfully submitted that claims 6 and 12 are patentable over Chen and Joiner at least for the same reasons their base claims are patentable.

Claim 6 is further patentable over Chen and Joiner at least for reciting: "wherein processing the data in the interception node comprises scanning the data for computer

viruses." As noted in the last office action, Chen does not disclose scanning data for computer viruses in the interception node. However, the last office action suggests that it would have been obvious to use the teachings of Joiner to perform virus scanning in Chen's authentication server ("interception node").

Joiner pertains to network analysis using an agent/host controller interface. Joiner col. 13, line 65 to col. 14, line 4, cited in the last office action, discusses scanning of network traffic for computer viruses in the host controllers 1002 (Joiner, col. 13, lines 54-64). Note, however, that host controllers 1002 are designed to cooperatively work with agents 900, not between peer nodes. That is, host controllers 1002 do not scan data being transferred between peer nodes in a peer-to-peer network. This is not surprising given that conventional data transfer between peer nodes are not scanned for viruses in transit, but rather in the peer nodes themselves. This is a type of problem specifically being addressed by claim 6 (e.g. see Specification, page 3, lines 3-6). Virus scanning of data in transit between two peer nodes is taught only in the present disclosure, not in any of the references of record.

Another problem with the Chen and Joiner combination is that data in Chen's authentication server are **encrypted**. In Chen, the encryption and decryption are performed in the sending and destination computers (Chen, FIG. 7, steps 106 and 109; col. 12, lines 11-26). Neither Chen nor Joiner discloses or suggests how virus scanning can be performed on encrypted data in a server between two peer nodes that perform local encryption and decryption. Therefore, data transferred between two peer nodes in Chen can only be scanned for viruses in either the sending or destination peer node, not in a host controller or authentication server.

Yet another problem with the Chen and Joiner combination is that in Chen, data to be transferred between two peer nodes do not pass through an intermediate server (see discussion with regard to claims 1 and 10 above). That is, in Chen, data are transferred directly between two peer nodes. There is no "interception node" where virus scanning can be performed. This is especially problematic as it requires both peer nodes to have antivirus software.

Claim 12 is similarly patentable over Chen and Joiner.

For at least the above reasons, it is respectfully submitted that claims 6 and 12 are patentable over Chen and Joiner.

Claim Rejection -- 35 U.S.C. § 103 (Chen and Yeager)

Claim 15 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Chen as applied to claim 10 and further in view of Yeager. The rejection is respectfully traversed.

The patentability of claim 10 over Chen has already been explained above. As previously explained, Chen does not disclose or suggest file transfer between two peer nodes passing through an interception node. This is not surprising considering conventional peer-to-peer communication is primarily directly between two peer nodes. Yeager does not add anything to Chen in regard to claim 10.

The last office action suggests it would have been obvious to combine the teachings of Chen and Yeager to allow for "querying a P2P server for location information of peer nodes involved in a transfer of the file; based on a response from the P2P server, identifying the second peer node as a node involved in the transfer of the file from the first peer node." This combination is suspect for several reasons. Firstly, the peer nodes in Chen include a shim for redirecting authentication information to the authentication server including the address of a destination peer node. Chen's VPN network does not need a P2P server for identifying nodes involved in a file transfer because such information is already provided by the shim to the authentication server in order to establish communication between peer-to-peer clients involved in the file transfer. A P2P server with location information of nodes involved in file transfer would thus be redundant in Chen's VPN network. Secondly, peer nodes in Chen will not be able to communicate with such a P2P server because communication between the peer nodes is encrypted and requires authentication services from the authentication server. Thirdly, Chen's peer nodes have no need for Yeager's trust mechanism because Chen's authentication server, the gist of Chen's invention, already authenticates the peer nodes.

Claim Rejection – 35 U.S.C. §103 (Yeager and Joiner)

Claims 17, 18, and 20 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Yeager as applied to claim 16 and further in view of Joiner.

The patentability of claim 16 over Yeager has already been explained above. Joiner does not add anything to Yeager in regard to claim 16. Claims 17, 18, and 20 depend on claim 16 and are thus patentable over Yeager and Joiner at least for the same reasons that claim 16 is patentable.

Claim 17 recites a data scanner configured to scan data passing through the interception node of claim 16. As noted in the last office action, Yeager does not disclose a data scanner configured to scan data passing through the interception node. Yeager does not have an interception node on which to do data scanning. This is not surprising as Yeager's trust mechanism is for peer-to-peer communication, and conventional peer-to-peer communication is directly between peers. The last office action suggests, however, that it would have been obvious to use Joiner's "interception node" to scan data transferred between two peer nodes in Yeager's peer-to-peer network. There are several problems with this conclusion. Firstly, conventional peer-to-peer data transfer does not involve an interception node between two peer nodes. Joiner's host controller ("interception node") does not stand between two peer nodes involved in peer-to-peer data transfer. Neither Joiner nor Yeager discloses or suggests that data being transferred between two peer nodes should be scanned in an interception node. Such a teaching is only taught in the present disclosure, **NOT** in Joiner or Yeager. Secondly, neither Yeager nor Joiner teaches or disclose how data in a peer-to-peer communication (which conventionally is a direct communication between two peer nodes) can be redirected through Joiner's host controller. The teaching on how to do so is in the present disclosure, not in Yeager or Joiner.

Claim 18 recites that the interception node of claim 1 is separate from a P2P server. As explained above in regard to claim 17, one of ordinary skill in the art would

not be motivated to modify Yeager's peer-to-peer network to include Joiner's "interception node."

Claim 20 recites that the data scanner of claim 17 is configured to scan the data for computer viruses. The patentability of claim 17 over Yeager and Joiner has already been explained. Conventional peer-to-peer data transfer does not involve an intermediary server, and thus do not involve virus scanning other than in the peers involved in the data transfer. Furthermore, there is no teaching on how Joiner's "interception node" can be placed in the data transfer path of Yeager's peer nodes involved in peer-to-peer communication.

Claim Rejection – 35 U.S.C. § 103 (Yeager and Chen)

Claim 21 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Yeager as applied to claim 16 and further in view of Chen.

The patentability of claim 16 over Yeager has already been explained above. Chen does not add anything to Yeager in regard to claim 16. Claim 21 depends on claim 16 and is thus patentable over Yeager and Chen at least for the same reasons that claim 16 is patentable.

Claim Rejection – 35 U.S.C. § 103 (Chen and Joiner)

Claim 22 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Chen and Joiner.

Claim 22 is patentable over Chen and Joiner at least for reciting: "transferring the file from a first peer node to an interception node, the file being originally intended to be transferred directly from the first peer node to a second peer node" and "scanning the file for viruses in the interception node. As previously explained, there are at least three problems with this combination. Firstly, in Chen, file transfer between two peer nodes do pass through an interception node. There is no interception node where the file can be scanned for viruses. Joiner's interception node is not and cannot be placed between two

of Chen's peer nodes. Secondly, files transferred between two of Chen's peers are encrypted and can only be decrypted in one of the peers. Thirdly, neither Chen nor Joiner discloses or suggests virus scanning of files in-transit between peer nodes. It is respectfully submitted that such virus scanning is not performed in the prior art (e.g. Chen, Joiner, and Yeager) because peer-to-peer file transfer is, by default, directly between peers. This is the main reason why peer-to-peer networks are established in the first place. Claim 22 breaks this convention to allow for virus scanning in a peer-to-peer file transfer without substantially impacting the use of such peer-to-peer networks.

For at least the above reasons, it is respectfully submitted that claim 22 is patentable over Chen and Joiner.

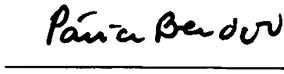
Conclusion

For at least the above reasons, it is believed that claims 1-22 are in condition for allowance. The Examiner is invited to telephone the undersigned at (408)436-2112 for any questions.

If for any reason an insufficient fee has been paid, the Commissioner is hereby authorized to charge the insufficiency to Deposit Account No. 50-2427.

Respectfully submitted,
En-Yi Liao

Dated: November 16, 2005



Patrick D. Benedicto, Reg. No. 40,909
Okamoto & Benedicto LLP
P.O. Box 641330
San Jose, CA 95164
Tel.: (408)436-2110
Fax.: (408)436-2114

CERTIFICATE OF MAILING			
I hereby certify that this correspondence, including the enclosures identified herein, is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below. If the Express Mail Mailing Number is filled in below, then this correspondence is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service pursuant to 37 CFR 1.10.			
Signature:	Patrick Benedicto		
Typed or Printed Name:	Patrick D. Benedicto	Dated:	November 16, 2005
Express Mail Mailing Number (*optional*):			